1) What is Active Directory

Active Directory is a directory service used to store information about the network resources across a domain.

An *Active Directory* (AD) structure is a hierarchical framework of objects. The objects fall into three broad categories - resources (e.g. printers , services (e.g. e-mail), and users (accounts, or users and groups). The AD provides information on the objects, organizes the objects, controls access, and sets security.

2) What are FSMO Roles? Explain Each Role

Windows 2000/2003 Multi-Master Model

A multi-master enabled database, such as the Active Directory, provides the flexibility of allowing changes to occur at any DC in the enterprise, but it also introduces the possibility of conflicts that can potentially lead to problems once the data is replicated to the rest of the enterprise. One way Windows 2000/2003 deals with conflicting updates is by having a conflict resolution algorithm handle discrepancies in values by resolving to the DC to which changes were written last (that is, "the last writer wins"), while discarding the changes in all other DCs. Although this resolution method may be acceptable in some cases, there are times when conflicts are just too difficult to resolve using the "last writer wins" approach. In such cases, it is best to prevent the conflict from occurring rather than to try to resolve it after the fact.

For certain types of changes, Windows 2000/2003 incorporates methods to prevent conflicting Active Directory updates from occurring.

Windows 2000/2003 Single-Master Model

To prevent conflicting updates in Windows 2000/2003, the Active Directory performs updates to certain objects in a single-master fashion.

In a single-master model, only one DC in the entire directory is allowed to process updates. This is similar to the role given to a primary domain controller (PDC) in earlier versions of Windows (such as Microsoft Windows NT 4.0), in which the PDC is responsible for processing all updates in a given domain.

In a forest, there are five FSMO roles that are assigned to one or more domain controllers. The five FSMO roles are

Schema Master:

The schema master domain controller controls all updates and modifications to the schema. Once the Schema update is complete, it is replicated from the schema master to all other DCs in the directory. To update the schema of a forest, you must have access to the schema master. There can be only one schema master in the whole forest.

Domain naming master:

The domain naming master domain controller controls the addition or removal of domains in the forest. This DC is the only one that can add or remove a domain from the directory. It can also add or remove cross references to domains in external directories. There can be only one domain naming master in the whole forest.

Infrastructure Master:

When an object in one domain is referenced by another object in another domain, it represents the reference by the GUID, the SID (for references to security principals), and the DN of the object being referenced. The infrastructure FSMO role holder is the DC responsible for updating an object's SID and distinguished name in a cross-domain object reference. At any one time, there can be only one domain controller acting as the infrastructure master in each domain.

Note: The Infrastructure Master (IM) role should be held by a domain controller that is not a Global Catalog server (GC). If the Infrastructure Master runs on a Global Catalog server it will stop updating object information because it does not contain any references to objects that it does not hold. This is because a Global Catalog server holds a partial replica of every object in the forest. As a result, cross-domain object references in that domain will not be updated and a warning to that effect will be logged on that DC's event log. If all the domain controllers in a domain also host the global catalog, all the domain controllers have the current data, and it is not important which domain controller holds the infrastructure master role.

3) **Relative ID (RID) Master:**

The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain. When a DC creates a security principal object such as a user or group, it attaches a unique Security ID (SID) to the object. This SID consists of a domain SID (the same for all SIDs created in a domain), and a relative ID (RID) that is unique for each security principal SID created in a domain. Each DC in a domain is allocated a pool of RIDs that it is allowed to assign to the security principals it creates. When a DC's allocated RID pool falls below a threshold, that DC issues a request for additional RIDs to the domain's RID master. The domain RID master responds to the request by retrieving RIDs from the domain's unallocated RID pool and assigns them to the pool of the requesting DC. At any one time, there can be only one domain controller acting as the RID master in the domain.

4) What is a Global Catalog

The Global Catalog (GC) has two primary functions. First, it acts as a domain controller that stores object data and manages queries about objects and their most common attributes (called the Global Catalog Partial Attribute Set, or PAS). Second, it provides data that permits network logon. In single domain controller environments, the Active Directory and GC reside on the same server. Where multiple domain controllers exist, as we discuss later, it is often advisable to move the GC to its own dedicated domain controller. All domain trees have a GC, and must reside on a domain controller.

5) What are Group Policies

Group policies are used by administrators to configure and control user environment settings. Group Policy Objects (GPOs) are used to configure group policies which are applied to sites, domains, and organizational units (OUs).

6) What is the difference between a Domain and Workgroup

Windows has two modes of operation - Workgroup and Domain. Depending on the environment that your computer is in, you will be running in one of these two modes. Most home and small business environments will be Workgroup, and most mid- to large businesses will run in domain mode. There are different features and capabilities depending on each, and each serve a purpose

Workgroups can be best understood as a loosely connected group of computers. They rely on each other for nothing, but they are there to share resources should the need arise. There is no centralized management and so there is a low barrier to use. By default, Windows XP is in this mode.

Domains, on the other hand, provide centralized management and security. User access is controlled from a separate server called a domain controller and there is a "trust" built between systems in a domain. There are much more robust differences as well.

Workgroup

A workgroup is best understood as a peer-to-peer network. That is, each computer is sustainable on its own. It has its own user list, it's own access control and its own resources. In order for a user to access resources on another workgroup computer, that exact user must be setup on the other computer.

In addition, workgroups offer little security outside of basic access control. Windows "share permissions" are very basic and do not offer any kind of granularity for "who" can access "what", etc. Workgroups are more than adequate, though, for most small business and home use.

Domain

A domain is a trusted group of computers that share security, access control and have data passed down from a centralized domain controller server or servers. Domain Controllers handle all aspects of granting users permission to login. They are the gatekeeper. In addition, most modern domains use Active Directory which allows and even more centralized point for software distribution, user management and computer controls.

7) What is the relationship between tree and a forest

Forests, trees, and domains

The framework that holds the objects is viewed at a number of levels. At the top of the structure is the Forest - the collection of every object, its attributes and rules (attribute syntax) in the AD. The forest holds one or more transitive, trust-linked Trees. A tree holds one or more Domains and domain trees, again linked in a transitive trust hierarchy. Domains are identified by their DNS name structure, the namespace. A domain has a single DNS name.

The objects held within a domain can be grouped into containers called Organizational Units (OUs). OUs give a domain a hierarchy, ease its administration, and can give a semblance of the structure of the AD's company in organizational or geographical terms. OUs can contain OUs - indeed, domains are containers in this sense - and can hold multiple nested OUs. Microsoft recommends as few domains as possible in AD and a reliance on OUs to produce structure and improve the implementation of policies and administration. The OU is the common level at which to apply group policies , which are AD objects themselves called Group Policy Objects (GPOs), although policies can also be applied to domains or sites (see below). The OU is the lowest level at which administrative powers can be delegated.

As a further subdivision AD supports the creation of *Sites*, which are physical, rather than logical, groupings defined by one or more IP subnets. Sites distinguish between locations connected by low-speed (e.g. WAN , VPN) and high-speed (e.g. LAN) connections. Sites can contain one or more domains and domains can contain one or more sites. This is important to control network traffic generated by replication.

The actual division of the company's information infrastructure into a hierarchy of one or more domains and top-level OUs is a key decision. Common models are by business, by geographical location, or by IT roles. These models are also often used in combination.

8) What is the file name of Active directory and where is it stored

File name : NTDS.DIT Location :

%SystemRoot%**ntds**

9) What are the different types of backups explain them

The Backup utility supports five methods of backing up data on your computer or network.

Copy backup

A copy backup copies all the files you select, but does not mark each file as having been backed up (in other words, the archive attribute is not cleared). Copying is useful if you want to back up files between normal and incremental backups because copying does not affect these other backup operations.

Daily backup

Daily backup copies all the files that you select that have been modified on the day the daily backup is performed. The backed-up files are not marked as having been backed up (in other words, the archive attribute is not cleared).

Differential backup

A differential backup copies files that have been created or changed since the last normal or incremental backup. It does not mark files as having been backed up (in other words, the archive attribute is not cleared). If you are performing a combination of normal and differential backups, restoring files and folders requires that you have the last normal as well as the last differential backup.

Incremental backup

An incremental backup backs up only those files that have been created or changed since the last normal or incremental backup. It marks files as having been backed up (in other words, the archive attribute is cleared). If you use a combination of normal and incremental backups, you will need to have the last normal backup set as well as all incremental backup sets to restore your data.

Normal backup

A normal backup copies all the files you select and marks each file as having been backed up (in other words, the archive attribute is cleared). With normal backups, you only need the most recent copy of the backup file or tape to restore all of the files. You usually perform a normal backup the first time you create a backup set.

Backing up your data using a combination of normal backups and incremental backups requires the least amount of storage space and is the quickest backup method. However, recovering files can be time-consuming and difficult because the backup set might be stored on several disks or tapes.

10) What is the difference between NTFS and FAT file system

file allocation table. FAT is ancient in computer terms. Because of its age, most operating systems-including Windows NT, Windows 98, MacOS, and some versions of UNIX-offer support for FAT.

Microsoft created the new technology file system (NTFS) to compensate for the features it felt FAT lacked. These features include increased fault tolerance, enhanced security, and so on.

Compatibility

Before you decide which type of file system to use on a partition, you must consider compatibility. If multiple operating systems will access the partition, you must use a file system that all operating systems can read. Usually, this means using FAT, because of its universal compatibility. Only Windows NT supports NTFS partitions.

Keep in mind, however, that this limitation applies only to the local machine. For example, if Windows NT and Windows 98 are loaded on the same machine and both operating systems require access to a common partition, you must format that partition as FAT. However, if Windows NT is the only operating system on the PC, you can format the partition as NTFS, even if computers running other operating systems will access the partition across the network.

Volume size

Another determining factor is the physical size of your partition. FAT supports partition sizes only up to 2 GB. If your partition size is larger than 2 GB, you must either format it as NTFS or break it into smaller partitions. Keep in mind that NTFS has more overhead than FAT. If your partition size is smaller than 200 MB, you should use FAT to avoid losing a major chunk of disk space to the overhead associated with NTFS. The maximum size of an NTFS partition is 16 EB (exabytes-an exabyte is 2^64 bytes, or 1,024 terabytes).

Fault tolerance

Once you've considered your partition size and compatibility issues, you have some flexibility in determining which file system is right for you. When making this decision, you should consider fault tolerance. Windows NT offers software support for several alternate disk-access methods that increase speed and/or fault tolerance. These options include disk striping and disk striping with parity. Many of these options require NTFS. If you're planning to use a hardware-based stripe set, you can use either file system.

Even without these advanced fault-tolerant options, NTFS includes built-in fault-tolerant capabilities well beyond the capabilities of FAT. For example, when NTFS writes a change to the hard disk, it makes a record of the change in a log file. In the event of a power failure or a disk error, Windows NT can use these log files to repair your data.

NTFS also repairs hard disk errors automatically without displaying an error message. When Windows NT writes a file to an NTFS partition, it keeps a copy of the file in memory. It then reads back the file to make sure it matches the copy stored in memory. If the copies don't match, Windows NT marks that section of the hard disk as corrupted and won't try to use it again. It then uses the copy of the file stored in memory to rewrite the file to an alternate location on the hard disk.
The FAT file system doesn't offer any of these safety features. While FAT does maintain two copies of the file-allocation table, in case one copy is damaged, it's incapable of automatically fixing errors. Instead, you must run a utility such as Scandisk.

Security

As we mentioned before, NTFS has a built-in security system. You can grant various permissions to directories and to individual files. These permissions protect files and directories locally and remotely. For example, if someone were to sit down at a PC containing restricted files, NTFS would protect those files.

If you're using FAT, you're dependent on share permissions for security. Share permissions will protect a file across the network, but they offer no local protection. A person trying to access restricted files could simply sit down at the local PC and gain full access to these files. Another disadvantage to share permissions is that they can be messy to manage. Suppose you have hundreds of users on a server, each with his or her own directories. You could potentially end up with hundreds of shares-and some of them may overlap, which creates additional complications.

File compression

Another advantage to NTFS is its native support for file compression. NTFS compression is much better than its predecessors. It offers you the chance to compress individual files and directories of your choice. Because it compresses individual files, a minor hard disk problem won't foul up your compression scheme and make you lose everything. Compressing individual files and directories also lets you limit compression to seldom-used files. By doing so, you won't slow your operating system by making it decompress files each time it needs to access them.

The system partition

This article may seem to say that NTFS is superior to FAT and that unless you have a small partition or need compatibility with other operating systems, you should always use NTFS. However, this isn't the case.

As we mentioned earlier, NTFS partitions are accessible only via Windows NT. If you have a fatal error with Windows NT, you can't simply boot a system disk to a command prompt and fix a problem on an NTFS partition. To get around this problem, Microsoft recommends installing a second copy of Windows NT on your hard disk and using this copy to repair problems that occur on NTFS partitions.

Unfortunately, this method has some serious drawbacks. For starters, a second copy of Windows NT could consume up to 150 MB, depending on which options you choose to load. Second, during the boot process, both copies share common files. Therefore, if your system partition (the partition your PC boots from) is formatted as NTFS and has a problem, you may not be able to boot either copy of Windows NT to fix the problem. While you may think the odds of a system partition error are slim, remember that many changes you might make to your disk partitions result in having to manually update the Boot.ini file. If you incorrectly update this file, Windows NT will become unbootable. Since this is an initial boot file on the system partition, every installed copy of Windows NT would share this file.

A better solution is to format your system partition as FAT. If you're concerned about security, simply make the system partition small and don't place anything other than the Windows NT system files on it. Remember, a FAT partition is safe from a security standpoint, as long as no unauthorized person has physical access to the machine.

11)Converting to NTFS

If you've read this article and wish you could use NTFS on some of your partitions that already contain data, you can easily convert a partition to NTFS. To do so, open an MS-DOS Prompt window and type the following command:

CONVERT drive: /FS:NTFS

For example, if you want to convert your D drive to NTFS, you'd replace the word *drive* with the letter *D*, as follows:

CONVERT D: /FS:NTFS

12) How do you install Active Directory

Procedure

To install Active Directory on Windows Server 2003

1. Click **Start**, click **Run**, type ***dcpromo***, and then click **OK**.
2. On the first page of the Active Directory Installation Wizard, click **Next**.

> **Note:**
>
> If this is the first time you have installed Active Directory, you can click **Active Directory Help** to learn more about Active Directory before clicking **Next**.

3. On the next page of the Active Directory Installation Wizard, click **Next**.
4. On the **Domain Controller Type** page, click **Domain Controller for a new domain**, and then click **Next**.
5. On the **Create New Domain** page, click **Domain in a new forest**, and then click **Next**.
6. On the **New Domain Name** page, in the **Full DNS name for new domain** box, type ***corp.contoso.com***, and then click **Next**.
7. On the **Database and Log Folders** page, accept the defaults in the **Database folder** box and the **Log folder** box, and then click **Next**.
8. On the **Shared System Volume** page, accept the default in the **Folder location** box, and then click **Next**.
9. On the **DNS Registration Diagnostics** page, click **Install and configure the DNS server on this computer and set this computer to use this DNS server as its preferred DNS Server**, and then click **Next**.
10. On the **Permissions** page, click **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**, and then click **Next**.
11. On the **Directory Services Restore Mode Administrator Password** page, enter a password in the **Restore Mode Password** box, retype the password to confirm it in the **Confirm password** box, and then click **Next**.
12. On the **Summary** page, confirm the information is correct, and then click **Next**.
13. When prompted to restart the computer, click **Restart now**.

13)EFS and DFS?

The Encrypting File System (EFS) on Microsoft Windows is a file system filter that provides filesystem-level encryption and was introduced in version 3.0 of NTFS[1]. The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.

Distributed File System (DFS) is a set of client and server services that allow an organization utilizing Microsoft Windows servers to organize many distributed SMB file shares into a distributed file system. DFS provides location transparency and redundancy to improve data availability in the face of failure or heavy load by allowing shares in multiple different locations to be logically grouped under one folder, or DFS root.

14) What is DNS?

The Domain Name System (DNS) is an integral part of client/server communications in Internet Protocol (IP) networks. DNS is a distributed database that is used in IP networks to translate, or resolve, computer names into IP addresses.

DNS uses a client/server model in which the DNS server contains information about a portion of the DNS namespace and provides this information to clients. A DNS client queries a DNS server for information about the DNS namespace. This server can, in turn, query other DNS servers to provide an answer to the query from the client.

When a DNS server receives a DNS request, it attempts to locate the requested information in its own database. If the request fails, further communication with other DNS servers is necessary.

Query Types

There are two types of queries that can be performed in DNS:

- *Iterative*. A query made from a client to a DNS server in which the server returns the best answer that it can provide based on its cache or zone data. If the queried server does not have an exact match for the request, it provides a pointer to an authoritative server in another level of the domain namespace.

  The client then queries the authoritative server to which it was referred. The client continues this process until it locates a server that is authoritative for the requested name or until an error occurs or a time-out condition is met.

- *Recursive*. A query made from a client to a DNS server in which the server assumes the full workload and responsibility for providing a complete answer to the query. The server will then perform separate iterative queries to other servers (on behalf of the client) to assist in answering the recursive query.

Zone type	Description
Standard primary	Contains a read/write version of the zone file that is stored in a standard text file. Any changes to the zone are recorded in that file.
Standard secondary	Contains a read-only version of the zone file that is stored in a standard text file. Any changes to the zone are recorded in the primary zone file and replicated to the secondary zone file. Create a standard secondary zone to create a copy of an existing zone and its zone file. This allows the name resolution workload to be distributed among multiple DNS servers.
Active Director y integrated	Stores the zone information in Active Directory, rather than a text file. Updates to the zone occur automatically during Active Directory replication. Create an Active Directory integrated zone to simplify planning and configuration of a DNS namespace. You do not need to configure DNS servers to specify how and when updates occur, because Active Directory maintains zone information.

15) What is DHCP?

Dynamic Host Configuration Protocol (**DHCP**) is a network application protocol used by devices (*DHCP clients*) to obtain configuration information for operation in an Internet Protocol network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual intervention.

DHCP discovery

The client broadcasts on the physical subnet to find available servers. Network administrators can configure a local router to forward DHCP packets to a DHCP server on a different subnet. This client-implementation creates a UDP packet with the broadcast destination of 255.255.255.255 or subnet broadcast address.

A client can also request its last-known IP address (in the example below, 192.168.1.100). If the client is still in a network where this IP is valid, the server might grant the request. Otherwise, it depends whether the server is set up as authoritative or not. An authoritative server will deny the request, making the client ask for a new IP immediately. A non-authoritative server simply ignores the request, leading to an implementation-dependent timeout for the client to give up on the request and ask for a new IP address.

DHCP offers

When a DHCP server receives an IP lease request from a client, it reserves an IP address for the client and extends an IP lease offer by sending a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

The server determines the configuration, based on the client's hardware address as specified in the CHADDR field. Here the server, 192.168.1.1, specifies the IP address in the YIADDR field.

DHCP requests

A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer and broadcast a DHCP request message. Based on Transaction ID field in the request, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

DHCP acknowledgement

When the DHCP server receives the DHCPREQUEST message from the client, the configuration processes enters its final phase. The acknowledgement phase involves sending a DHCPACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is complete

16) When do I run a Repair?

When the C:\windows\system32\ files are missing or corrupt

17) Protocols used by VPN or RRAS ?

Point-to-Point Tunneling Protocol (PPTP)

Several corporations worked together to create the PPTP specification. People generally associate PPTP with Microsoft because nearly all flavors of Windows include built-in

client support for this protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.

Layer Two Tunneling Protocol (L2TP)

The original competitor to PPTP for VPN tunneling was L2F, a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create a new standard called L2TP. Like PPTP, L2TP exists at the data link layer (Layer Two) in the OSI model -- thus the origin of its name.

Internet Protocol Security (IPsec)

IPsec is actually a collection of multiple related protocols. It can be used as a complete VPN protocol solution or simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (Layer Three) of the OSI model.

18) Different Groups in Windows?

A *domain local group* is a security or distribution group that can contain universal groups, global groups, other domain local groups from its own domain, and accounts from any domain in the forest. You can give domain local security groups rights and permissions on resources that reside only in the same domain where the domain local group is located.

A *global group* is a group that can be used in its own domain, in member servers and in workstations of the domain, and in trusting domains. In all those locations, you can give a global group rights and permissions and the global group can become a member of local groups. However, a global group can contain user accounts that are only from its own domain.

A *universal group* is a security or distribution group that contains users, groups, and computers from any domain in its forest as members. You can give universal security groups rights and permissions on resources in any domain in the forest. Universal groups are not supported.

If you plan to use one domain for all your servers and no Wide Area Network (WAN) exists, we recommend that you use domain local groups. For a local domain, the global catalog is not used.

19) What Logical and Physical Structure of AD ?

Logical : Domain, Tree, Forest, OU

Physical : Domain Controller and Sites

20) How do I install Roles :-

Add remove Program or Manage your server

Some Roles : AD, DNS, DHCP, File server, Print Server, Terminal Server, VPN

21) What is a firewall?

A **firewall** is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices which is configured to permit or deny computer based application upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

22) What is a Proxy server?

proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it 'caches' responses from the remote server, and returns subsequent requests for the same content directly.

23) Why do I share folders?

To share resources or data

24) How to I map a drive?

Right Click computer> Map network drive and show the path of the shared folder

My computer> tools> Map network drive

25)What is IIS ?

Internet Information Services (**IIS**) - formerly called **Internet Information Server** - is a web server application and set of feature extension modules created by Microsoft for use with Microsoft Windows. It is the world's second most popular web server in terms of overall websites behind the industry leader

26) Boot sequence of PC

When you hit the power button on your computer a whole lot of stuff happens. We call this the boot process. In the days when I first started using computers there was literally a "boot disk", a floppy (5.25" not a 3.5") disk that told the system where to go and what to do so that the operating system would start up. Since then the boot sequence has become somewhat more complicated. So let me take you thru the steps the computer takes to get started. For my example I'm going to use a Windows XP system.

1. First is the POST, this stands for Power On Self Test, for the computer. This process tests memory as well as a number of other subsystems. You can usually monitor this as it runs each test. After that is complete the system will run POST for any device that has a BIOS (Basic Input-Output System). An AGP has its own BIOS, as do some network cards and various other devices.
2. Once the POST is complete and the BIOS is sure that everything is working properly, the BIOS will then attempt to read the MBR (Master Boot Record). This is the first sector of the first hard drive (called the Master or HD0). When the MBR takes over it means that Windows is now in control.
3. The MBR looks at the BOOT SECTOR (the first sector of the active partition). That is where NTLDR is located, NTLDR is the BOOT LOADER for Windows XP. NTLDR will allow memory addressing, initiate the file system, read the boot.ini and load the boot menu. NTLDR has to be in the root of the active partition as do NTDETECT.COM, BOOT.INI, BOOTSECT.DOS (for multi-OS booting) and NTBOOTDD.SYS (if you have SCSI adapters)
4. Once XP is selected from the Boot Menu, NTLDR will run NTDETECT.COM, BOOT.INI and BOOTSECT.DOS to get the proper OS selected and loaded. The system starts in 16-bit real mode and then moves into 32-bit protected mode.
5. NTLDR will then load NTOSKRNL.EXE and HAL.DLL. Effectively, these two files are windows XP. They must be located in %SystemRoot%System32.
6. NTLDR reads the registry, chooses a hardware profile and authorizes device drivers, in that exact order.

At this point NTOSKRNL.EXE takes over. It starts WINLOGON.EXE that in turn starts LSASS.EXE, this is the program that display the Logon screen so that you can logon

27) MBR (master boot record)

A **master boot record** (**MBR**), or **partition sector**, is the 512-byte boot sector that is the first sector on a partitioned Hard drive.

28) What options u have in manage (right click my comp -> manage)

System Tools

- Event Viewer
- Shared folder
- Local users and Group
- Performance Logs and Alerts
- Device Manager

Storage

- Removable Storage
- Disk Defragmenter.
- Disk Management

Services and Applications

- Services
- WMI
- Control
- Indexing Services

29) Different Servers???

WinNT/2000/2003/2008

30) Can Win Home Edition be added in a Domain?If no Why?

No,

This is NOT a complete list; I am just listing the features related to networking:

Windows XP Home Edition	**Windows XP Professional Edition**		
	User management	Limited to 2 security levels, no policies	Full User Management and Security Policies
	Workgroup networking/ Joining domains	Limited to Workgroup network (unable to join a domain)	Workgroup networking and able to join a Domain

	Security on sharing disks and folders	no security, everybody has access to shared data	Full security based on User Management
	Limit of simultaneous file-sharing connections	max 5 simultaneous file-sharing connections	max 10 simultaneous file-sharing connections
	Security of disks and folders (NTFS drives)	limited Security, made difficult to use	Full Disk/Folder Security based on User Management
Group Policy Editor	not included	Included	
	Remote Desktop Access	not included.	Remote Desktop Access
	Backup Program	only included via VALUEADD	Included
	ASR Automatic System Recovery	not included	Included

The lack of the possibility to join a domain and the lack of securing a shared network resource will prevent the use of the XP Home edition in most office networks, even in configurations where Windows95/98/ME could be used.

31) why does safe mode have a black background?

Video card is disabled or not loaded

32)What is RAID?

RAID (originally **redundant array of inexpensive disks**, now also known as **redundant array of independent disks**) refers to a data storage scheme using multiple hard drives to share or replicate data among the drives. Depending on the version chosen, the benefit of RAID is one or more of increased data integrity , fault-tolerance , throughput or capacity compared to single drives. In its original implementations, its key advantage was the ability to combine multiple low-cost devices using older technology into an array that offered greater capacity, reliability, speed, or a combination of these things, than was affordably available in a single device using the newest technology.

Standard RAID levels

A quick summary of the most commonly used RAID levels:

RAID 0 with is 2 PHYSICAL hard drives put together to make one big drive. Their upside is super fast read write time, the down side would be no fault tolerance so when you lose a drive it can be an expensive proposition getting your data back.

RAID 1 This is the Mirrored Set we all hear about. it is 2 PHYSICAL drive put together so that you have an exact duplicate of the main drive. The upside is that face that you always have a backup, downside would be that it is slow for reading and writing because it has to propagate the data on both drive.

RAID 5 This is the ARRAY everyone think about when you say you have a RAID. This is multiple disks (3 or more) put together to make a fault tolerant drive. The idea being that it will write data across all drives duplicating the data in small pieces as it goes. So in theory you can lose a drive and still be running. This kind of array is faster then RAID 1 but extremely temperamental. It requires a technician with some expertise to monitor and maintain because drives can fall out of the array all of the time.

33) System requirements for different servers?

The following table lists the system requirements for **Windows Server 2003 Standard Edition.**

Component	Requirement
Computer and processor	PC with a 133-MHz processor required; 550-MHz or faster processor recommended (Windows Server 2003 Standard Edition supports up to four processors on one server)
Memory	128 MB of RAM required; 256 MB or more recommended; 4 GB maximum
Hard disk	1.25 to 2 GB of available hard-disk space
Drive	CD-ROM or DVD-ROM drive

The following table lists the system requirements for **Windows Server 2003 Enterprise Edition**

Component	Requirement
Computer and processor	133-MHz or faster processor for x86-based PCs; 733-MHz for Itanium-based PCs; up to eight processors supported on either the 32-bit or the 64-bit version
Memory	128 MB of RAM minimum required; maximum: 32 GB for x86-based PCs with the 32-bit version and 64 GB for Itanium-based PCs with the 64-bit version
Hard disk	1.5 GB of available hard-disk space for x86-based PCs; 2 GB for Itanium-based PCs; additional space is required if installing over a network
Drive	CD-ROM or DVD-ROM drive
Display	VGA or hardware that supports console redirection required

The following table lists the system requirements for **Windows Server 2003 Datacenter Edition**

Component	Requirement
Computer and processor	Minimum: 400 MHz processor for x86-based computers or 733 MHz for Itanium-based computers; recommended: 733 MHz processor
Memory	Minimum: 512 MB of RAM; recommended: 1 GB of RAM
Hard disk	1.5 GB hard-disk space for x86-based computers; 2.0 GB for Itanium-based computers
Other	Minimum: 8-way capable multiprocessor machine required; maximum: 64-way capable multiprocessor machine supported

The following table lists the system requirements for **Windows Server 2003 Web Edition**

Component	Requirement
Computer and processor	133-MHz processor (550 MHz recommended)
Memory	128 MB of RAM (256 MB recommended; 2 GB maximum)
Hard disk	1.5 GB of available hard-disk space

34) How much Ram does win server 2003 standard edition support?

>4 GB

35) Which logs u have in event viewer, etc..

Application: All Application Related errors

System: All Service related events

Security: Logon, Log off related events

36) What is msconfig ?

Microsoft System Configuration Utility to manage the Startup Behaviour.

37) What are the Switches in Boot.ini in msconfig

/safeboot:minimal

/noguiboot

/bootlog

/Basevideo

/sos

38) What is NAT, how it work?[1]

NAT is like the receptionist in a large office. Let's say you have left instructions with the receptionist not to forward any calls to you unless you request it. Later on, you call a potential client and leave a message for them to call you back. You tell the receptionist that you are expecting a call from this client and to put them through. The client calls the main number to your office, which is the only number the client knows. When the client tells the receptionist who they are looking for, the receptionist checks a lookup table that matches up the person's name and extension. The receptionist knows that you requested this call, therefore the receptionist forwards the caller to your extension.

Developed by Cisco, Network Address Translation is used by a device (firewall, router or computer) that sits between an internal network and the rest of the world. NAT has many forms and can work in several ways:

39) what is OU?

Organizational Units", are administrative-level containers on a computer network that allow network administrators to organize groups of users together so that any changes, security privileges or any other administrative tasks could be accomplished more efficiently.

A network administrator will typically create organizational units that resemble their company's business organization. An OU can be set up for each department. Within that department OU, there could be subsets, or objects that represent users, groups, customers, partners, vendors or even computers and printers on the network.

Applying a set of policies or restrictions to an organizational unit applies it to all subsets within that organization unit. An object, placed into a new organization unit, inherits all the policies and rights associated with that organizational unit.

Organizational Units are used on systems as a form of identity management, a method of technology used to automate various administrative applications such as password synchronization, resetting passwords, user provisioning, meta directories, and consolidated reporting and auditing.

40) Default least period of DHCP ? Manual and Automatic Lease Renewal ?

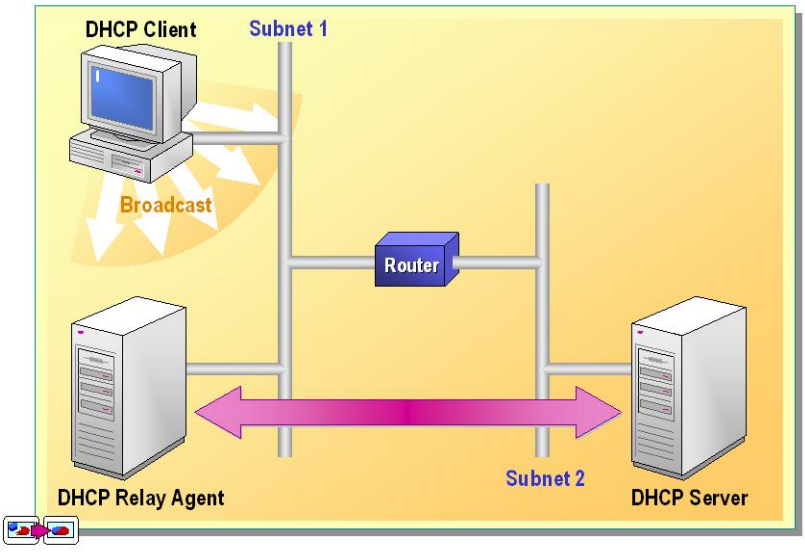
Manaul : ipconfig /release & then ipconfig /renew

Automatic : A DHCP client automatically attempts to renew its lease when 50 percent of the lease duration expires. To attempt a lease renewal, the DHCP client sends a DHCPREQUEST message directly to the DHCP server from which it obtained the lease.

If the DHCP server is available, it renews the lease and sends the client a DHCPACK message with the new lease duration and any updated configuration parameters. The client updates its configuration when it receives the acknowledgment. If the DHCP server is unavailable, the client continues to use its current configuration parameters.

If a DHCP client cannot renew its lease at the 50 percent interval, the client continues to use its current configuration parameters. It then broadcasts a DHCPDISCOVER message to update its address lease when 87.5 percent of the current lease duration expires. At this stage, the DHCP client accepts a lease that is issued by any DHCP server.

41) What is DHCP relay Agent?



On a local subnet, a DHCP relay agent intercepts address request broadcast messages from the DHCP client and forwards them to a DHCP server on another subnet. The DHCP server responds to the relay agent by using a directed packet. The relay agent then broadcasts the response on the local subnet for the requesting client to use.

42) classes of IP

Short for **Internet Protocol**, **IP** is an address of a computer or other network device on a network using IP or TCP/IP . For example, the number "166.70.10.23" is an example of such an address. These addresses are similar to addresses used on houses and help data reach its appropriate destination on a network.

There are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B and C are commonly used. Each class allows for a range of valid IP addresses. Below is a listing of these addresses.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

43) what is MAC address..Mention the Bit?

In computer networking, a Media Access Control address (MAC address), Ethernet Hardware Address (EHA), hardware address, adapter address or physical address is a quasi-unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number.

Three numbering spaces, managed by the Institute of Electrical and Electronics Engineers (IEEE), are in common use for formulating a MAC address:

44)Explain Hub, Switch and Router:-

A **hub** is typically the least expensive, least intelligent, and least complicated of the three. Its job is very simple: anything that comes in one port is sent out to the others. That's it. Every computer connected to the hub "sees" everything that every other computer on the hub sees. The hub itself is blissfully ignorant of the data being transmitted. For years, simple hubs have been quick and easy ways to connect computers in small networks.

A **switch** does essentially what a hub does but more efficiently. By paying attention to the traffic that comes across it, it can "learn" where particular addresses are. For example, if it sees traffic from machine A coming in on port 2, it now knows that machine A is connected to that port and that traffic to machine A needs to only be sent to that port and not any of the others. The net result of using a switch over a hub is that most of the network traffic only goes where it needs to rather than to every port. On busy networks this can make the network significantly faster.

A **router** is the smartest and most complicated of the bunch. Routers come in all shapes and sizes from the small four-port broadband routers that are very popular right now to the large industrial strength devices that drive the internet itself. A simple way to think of a router is as a computer that can be programmed to understand, possibly manipulate, and route the data its being asked to handle. For example, broadband routers include the ability to "hide"

computers behind a type of firewall which involves slightly modifying the packets of network traffic as they traverse the device. All routers include some kind of user interface for configuring how the router will treat traffic. The really large routers include the equivalent of a full-blown programming language to describe how they should operate as well as the ability to communicate with other routers to describe or determine the best way to get network traffic from point A to point B.

45)Explain the Registry ?

The Windows registry is a directory which stores settings and options for the operating system for Microsoft Windows 32-bit versions, 64-bit versions, and Windows Mobile. It contains information and settings for all the hardware, operating system software, most non-operating system software, users, preferences of the PC, etc. Whenever a user makes changes to Control Panel settings, file associations, system policies, or most installed software, the changes are reflected and stored in the registry. The registry also provides a window into the operation of the kernel, exposing runtime information such as performance counters and currently active hardware

Keys and values

The following table lists the five keys in the registry.

Registry Key	Description
HKEY_CLASSES_ROOT	This key is where data on DLL files and applications is stored.
HKEY_CURRENT_USER	This key is where the current user's individual customizations are stored and tracked.
HKEY_LOCAL_MACHINE	This key contains information about all of the software installed on the computer. Virtually anything that the operating system might need to know about a particular application is stored here.
HKEY_USERS	This key is where all user data is stored. If multiple people use the same computer, all their user profiles are stored here. When a user logs on to the computer, the data is written to **HKEY_CURRENT_USER**.
HKEY_CURRENT_CONFIG	This key points to the current computer hardware configuration in the collection of configurations stored in **HKEY_LOCAL_MACHINE**. This enables the use of multiple computer hardware profiles.

46) Windows Advanced boot options:-

use a Safe Boot option, follow these steps:

Restart your computer and start pressing the F8 key on your keyboard. On a computer that is configured for booting to multiple operating systems, you can press the F8 key when the Boot Menu appears.
Select an option when the Windows Advanced Options menu appears, and then press ENTER.

When the Boot menu appears again, and the words "Safe Mode" appear in blue at the bottom, select the installation that you want to start, and then press ENTER.
Back to the top
Description of Safe Boot options

Safe Mode (SAFEBOOT_OPTION=Minimal): This option uses a minimal set of device drivers and services to start Windows.

Safe Mode with Networking (SAFEBOOT_OPTION=Network): This option uses a minimal set of device drivers and services to start Windows together with the drivers that you must have to load networking.

Safe Mode with Command Prompt (SAFEBOOT_OPTION=Minimal(AlternateShell)): This option is the same as Safe mode, except that Cmd.exe starts instead of Windows Explorer.
Enable VGA Mode: This option starts Windows in 640 x 480 mode by using the current video driver (not Vga.sys). This mode is useful if the display is configured for a setting that the monitor cannot display.

Note Safe mode and Safe mode with Networking load the Vga.sys driver instead.

Last Known Good Configuration: This option starts Windows by using the previous good configuration. Directory Service Restore Mode:

This mode is valid only for Windows-based domain controllers. This mode performs a directory service repair.

Debugging Mode: This option turns on debug mode in Windows. Debugging information can be sent across a serial cable to another computer that is running a debugger. This mode is configured to use COM2.
Enable Boot Logging: This option turns on logging when the computer is started with any of the Safe Boot options except Last Known Good Configuration. The Boot Logging text is recorded in the Ntbtlog.txt file in the %SystemRoot% folder.

Starts Windows Normally: This option starts Windows in its normal mode.
Reboot: This option restarts the computer.

Return to OS Choices Menu: On a computer that is configured to starting to more than one operating system, this option returns to the Boot menu.
An environment variable is set when you use one of the Safe Boot options. The environment variable is SAFEBOOT_OPTION. This variable is set to either Network or to Minimal.

The default Microsoft VGA driver is used for display at 640 x 480 resolution and in 16 colors. You must log on in all modes by a domain or by the local Security Accounts Manager, depending on which Safe Boot mode you select.

47) OSI layers

Characteristics of the OSI Layers

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers.

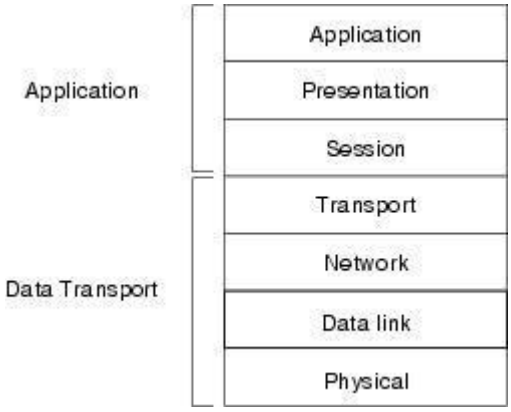
The *upper layers* of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with

software applications that contain a communications component. The term upper layer is sometimes used to refer to any layer above another layer in the OSI model.

The *lower layer*s of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example) and is responsible for actually placing information on the medium.

Figure 1-3 illustrates the division between the upper and lower OSI layers.

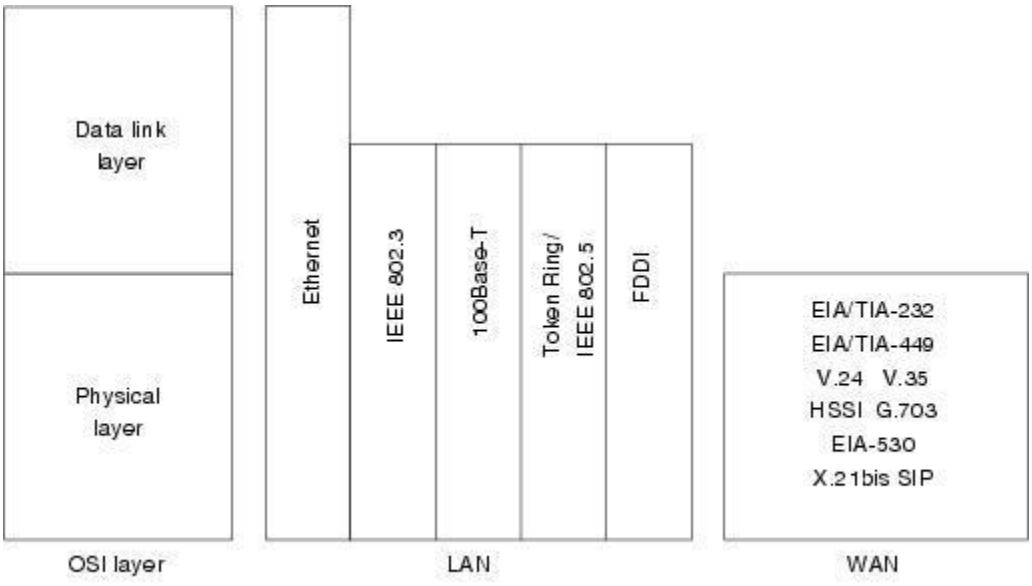
Figure 1-3 Two Sets of Layers Make Up the OSI Layers



OSI Model Physical Layer

The physical layer defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems. Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors. Physical layer implementations can be categorized as either LAN or WAN specifications. Figure 1-7 illustrates some common LAN and WAN physical layer implementations.

Figure 1-7 Physical Layer Implementations Can Be LAN or WAN Specifications

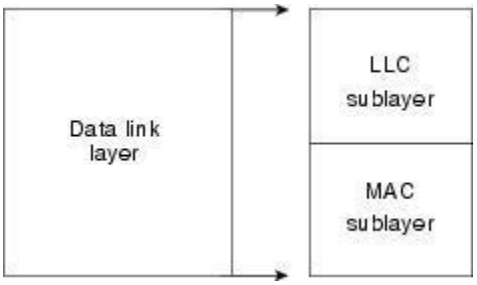


OSI Model Data Link Layer

The data link layer provides reliable transit of data across a physical network link. Different data link layer specifications define different network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control. Physical addressing (as opposed to network addressing) defines how devices are addressed at the data link layer. Network topology consists of the data link layer specifications that often define how devices are to be physically connected, such as in a bus or a ring topology. Error notification alerts upper-layer protocols that a transmission error has occurred, and the sequencing of data frames reorders frames that are transmitted out of sequence. Finally, flow control moderates the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time.

The Institute of Electrical and Electronics Engineers (IEEE) has subdivided the data link layer into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). Figure 1-8 illustrates the IEEE sublayers of the data link layer.

Figure 1-8 The Data Link Layer Contains Two Sublayers



The *Logical Link Control (LLC)* sublayer of the data link layer manages communications between devices over a single link of a network. LLC is defined in the IEEE 802.2 specification and supports both connectionless and connection-oriented services used by higher-layer protocols. IEEE 802.2 defines a number of fields in data link layer frames that enable multiple higher-layer protocols to share a single physical data link. The *Media Access Control (MAC)* sublayer of the data link layer manages protocol access to the physical network medium. The IEEE MAC specification defines MAC addresses, which enable multiple devices to uniquely identify one another at the data link layer.

OSI Model Network Layer

The network layer defines the network address, which differs from the MAC address. Some network layer implementations, such as the Internet Protocol (IP), define network addresses in a way that route selection can be determined systematically by comparing the source network address with the destination network address and applying the subnet mask. Because this layer defines the logical network layout, routers can use this layer to determine how to forward packets. Because of this, much of the design and configuration work for internetworks happens at Layer 3, the network layer.

OSI Model Transport Layer

The transport layer accepts data from the session layer and segments the data for transport across the network. Generally, the transport layer is responsible for making sure that the data is delivered error-free and in the proper sequence. Flow control generally occurs at the transport layer.

Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process. Multiplexing enables data from several applications to be transmitted onto a single physical link. Virtual circuits are established, maintained, and terminated by the transport layer. Error checking involves creating various mechanisms for detecting transmission errors, while error recovery involves acting, such as requesting that data be retransmitted, to resolve any errors that occur.

The transport protocols used on the Internet are TCP and UDP.

OSI Model Session Layer

The session layer establishes, manages, and terminates communication sessions. Communication sessions consist of service requests and service responses that occur between applications located in different network devices. These requests and responses are coordinated by protocols implemented at the session layer. Some examples of session-layer implementations include Zone Information Protocol (ZIP), the AppleTalk protocol that coordinates the name binding process; and Session Control Protocol (SCP), the DECnet Phase IV session layer protocol.

OSI Model Presentation Layer

The presentation layer provides a variety of coding and conversion functions that are applied to application layer data. These functions ensure that information sent from the application layer of one system would be readable by the application layer of another system. Some examples of presentation layer coding and conversion schemes include common data representation formats, conversion of character representation formats, common data compression schemes, and common data encryption schemes.

Common data representation formats, or the use of standard image, sound, and video formats, enable the interchange of application data between different types of computer systems. Conversion schemes are used to exchange information with systems by using different text and data representations, such as EBCDIC and ASCII. Standard data compression schemes enable data that is compressed at the source device to be properly decompressed at the destination. Standard data encryption schemes enable data encrypted at the source device to be properly deciphered at the destination.

Presentation layer implementations are not typically associated with a particular protocol stack. Some well-known standards for video include QuickTime and Motion Picture Experts Group (MPEG). QuickTime is an Apple Computer specification for video and audio, and MPEG is a standard for video compression and coding.

Among the well-known graphic image formats are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF). GIF is a standard for compressing and coding graphic images. JPEG is another compression and coding standard for graphic images, and TIFF is a standard coding format for graphic images.

OSI Model Application Layer

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.

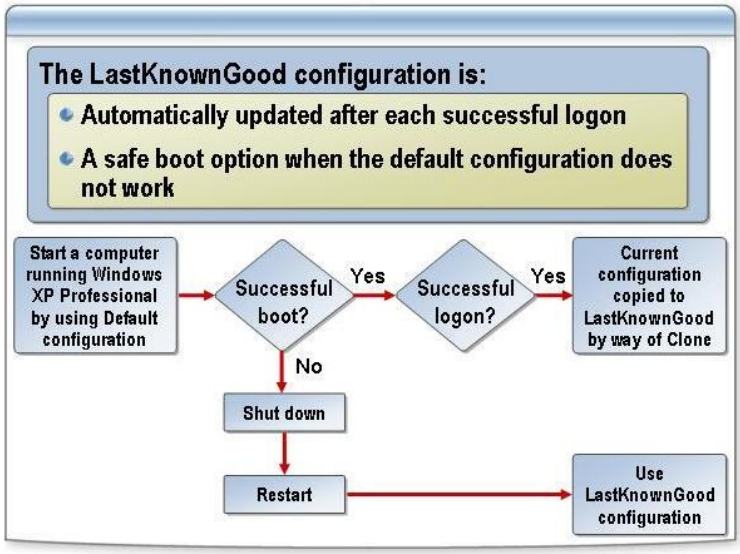
This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.

When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit.
When determining resource availability, the application layer must decide whether sufficient network resources for the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer. Some examples of application layer implementations include Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP).

48) Mention the hives of HKLM?

HKEY_LOCAL_MACHINE\HARDWARE
HKEY_LOCAL_MACHINE\SAM
HKEY_LOCAL_MACHINE\SECURITY
HKEY_LOCAL_MACHINE\SOFTWARE
HKEY_LOCAL_MACHINE\SYSTEM

49) How does LKGC work?



During the kernel initiation sequence of the boot process, the kernel copies the information in the **CurrentControlSet** to the **CloneControlSet**. After a successful logon, the information in the Clone is copied to the LastKnownGood configuration.

You usually start a computer by using the Default configuration. When you make a configuration change, the change is stored in the **CurrentContolSet**. When you shut down or restart the computer, the change is copied to the Default configuration.

If you make a configuration change, such as adding a device driver, and encounter problems when you restart the computer, your configuration changes may have damaged the Default configuration. In this case, you can use the LastKnownGood configuration to safely restart the computer. The next time that you log on, the Current configuration is copied to the Default configuration, which ensures that the Default configuration will start the computer the next time you restart it.

Problem	**Solution**
After you install a new device driver, Windows Server 2003 stops responding.	Use the LastKnownGood configuration during startup. The LastKnownGood configuration will not contain a reference to the new, and possibly defective, device driver.
You accidentally disable a critical device driver.	If a critical driver becomes disabled, use the LastKnownGood configuration during startup. Some critical drivers are configured to prevent users from accidentally disabling them. If these drivers are damaged, the computer automatically reverts to the LastKnownGood configuration the next time it starts

50) Different ways of installing the OS ?

- Interactive (or manual) setup relies on the Setup program in Windows Server 2003 and provides a method for carrying out an interactive installation or upgrade on a single computer. Interactive setup can be started by running Setup.exe, but also by running Winnt32.exe or Winnt.exe, both of which offer command-line options. The Setup program is also the basis for the automated installation technologies, including RIS, Sysprep, and unattended installation.

  Running Setup interactively is a simple way to accomplish a server installation or upgrade. The installation or upgrade can be carried out from the CD drive or across the network (after you copy the installation files that are on the product CD to a shared folder). In addition, interactive setup requires little preparatory work compared to automated installation, and does not require supplemental tools or programs. Also, interactive setup can be used to install an operating system on a computer that is not connected to a network.

- Unattended installation is an automated installation technology in Windows Server 2003 that you can use to install or upgrade an operating system with minimal user intervention. Unattended installation relies on the Setup program and an answer file to automate the setup process. An answer file is a simple text file that provides details about how to install and configure the operating system. To start an unattended installation, you run Winnt32.exe or Winnt.exe with a command-line parameter that specifies the answer file to use. Then, during the installation process, necessary information is obtained from instructions contained in the answer file instead of your responses to prompts

- Sysprep is an automated installation technology that you can use to install Windows Server 2003 and Microsoft Windows XP operating systems. The Sysprep tool is typically used in conjunction with a non-Microsoft disk imaging tool or Microsoft Windows Server 2003 Automated Deployment Services (ADS) to perform image-based installations.

  Image-based installation is a method of copying or cloning preconfigured operating systems (and, optionally, software applications) onto destination computers. After you set up a master installation — an installation with the operating system, software applications, and configuration settings that you want to install onto the destination computers in your organization, Sysprep prepares the master installation so that you can create a disk image; that

is, a functionally identical replica of the disk containing the master installation, that can be copied onto multiple computers.

Next, you use a disk-imaging program to create the disk image of the master installation. After you copy the disk image onto a destination computer and start the destination computer, a shortened version of the Setup program runs. The shortened version of Setup configures only user-specific and computer-specific settings, such as computer name, domain membership, and regional options. You can automate this last part of the setup process by using an answer file, a simple text file that instructs the Setup program how to configure the various operating system settings.

- Remote Installation Services (RIS) is an automated installation technology that can be used to install Windows Server 2003, Windows XP, and Microsoft Windows 2000 operating systems. RIS uses Pre-Boot Execution Environment (PXE) technology to enable client computers without an operating system to start up and connect remotely to a RIS server, which installs a supported operating system.

  You can use RIS to perform either CD-based installations or image-based installations. To perform CD-based installations you use the Remote Installation Services Setup (Risetup.exe) tool, which installs an operating system on a destination computer by using an answer file and the installation files that are on the product CD. To perform image-based installations you use the Remote Installation Preparation Wizard (Riprep.exe) tool, which is similar to the Sysprep tool and prepares a master installation for disk imaging.

UNC Universal Naming Convention
\\servername\shared name (It is used to access the shared folder)
MAC Media Access Control
PDC Primary Domain Controllers
BDC Backup Domain Controllers
SMP Symmetric Multi Processors
AMP Asymmetric Multi Processing
EFS Encrypted File System
FAT File Allocation Table
HCL Hardware Compatibility List
IIS Internet Information Service
LSA Local Security Authority
MMC Microsoft Management Console
OU Organizational Unit
RAS Remote Access Service
RDP Remote Desktop Protocol (used for Terminal Services)
RRAS Routing and Remote Access Service
SID Security Identifier
WINS Windows Internet Name Service
GUID Globally Unique identifier
IAS Internet Authentication Service
UPN User Principle Name (Username@domainname.com)
BIOS Basic Input Output System

Net BIOS Network Basic Input/Output System
ARP Address Resolution Protocol
DVD Digital Video Disk
GPO Group Policy Object (LGPO Local Group Policy Object)
IPsec Internet Protocol Security
ISP Internet Service Provider
NAT Network Address Translation
MBT Master Boot Record
USB Universal Serial Bus
POST Power On Self Test
SCSI Small Computer System Interface
SMTP Simple Mail Transfer Protocol
URL Uniform Resource Locator
RAID Redundant Array of Independent Disk
IDE Intelligent drive Electronics *or* Integrated Drive Electronics
FQDN Fully Qualified Domain Name (full computer name)
[computername.domainname.com]
OSPF Open Shortest Path First (these two are routing protocols)
RIP Routing Information Protocol
POP3 Post Office Protocol (used to receive the mails)
SMTP Simple Mail Transfer Protocol (Used to send the mails)
SMPS Switch Mode Power Supply
PING Packet Internet Groper
VNC Virtual Network Computing
EULA End User License Agreement
CAL Client Access License
TSCAL Terminal Services Client Access License
UPS Uninterruptible Power Supply
BIND Berkeley Internet Name Domain
PXE Pre boot eXecutable Environment
UDF Uniqueness Database file
LDAP Light weight Directory Access Protocol
ISDN Integrated Services Digital Network
VLSM Variable Length Subnet Mask
CIDR Classless Inter Domain Routing
IGMP Internet Group Management Protocol
FSMO Flexible Single Master Operations
APIPAAutomatic IP addressing
NetBEUI Net Bios Enhanced User Interface
UDP User Datagram Protocol
FTP File Transfer Protocol
Mbps Mega bits per second
Ntds.dit Nt directory services.directory information tree.
ICMP Internet Control message Protocol
IGMP Internet group Management Protocol
NNTP Network News Transfer Protocol
RADIUS Remote Authentication Dial In User service
SNMP Simple Network Management protocol

VPN Virtual Private Network
L2TP Layer2 Tunneling Protocol
PPTP Point to Point Tunneling Protocol
ADSI Active Directory Service Interfaces
SUS Software Update Service
SMS System Management Service
WUS Windows Update service
TFTP Trivial File Transfer Protocol

List of important port numbers
15 – Netstat
17- UDP
21 - FTP
23 - Telnet
25 - SMTP
42 - WINS
53 - DNS
67 - Bootp
68 - DHCP
80 - HTTP
88 - Kerberos
101 - HOSTNAME
110 - POP3
119 - NNTP
123 - NTP (Network time protocol)
139 - NetBIOS
161 - SNMP
180 - RIS
389 - LDAP (Lightweight Directory Access Protocol)
443 - HTTPS (HTTP over SSL/TLS)
520 - RIP
79 - FINGER
37 - Time
3389 - Terminal services
443 -SSL (https) (http protocol over TLS/SSL)
220 - IMAP3
3268 - AD Global Catalog
3269 - AD Global Catalog over SSL
500 -nternet Key Exchange, IKE (IPSec) (UDP 500)